ARMOR™

BETWEEN YOU AND THE THREAT

A Guide to

HIPAA compliance & risk management

A PROACTIVE APPROACH TO DATA SECURITY

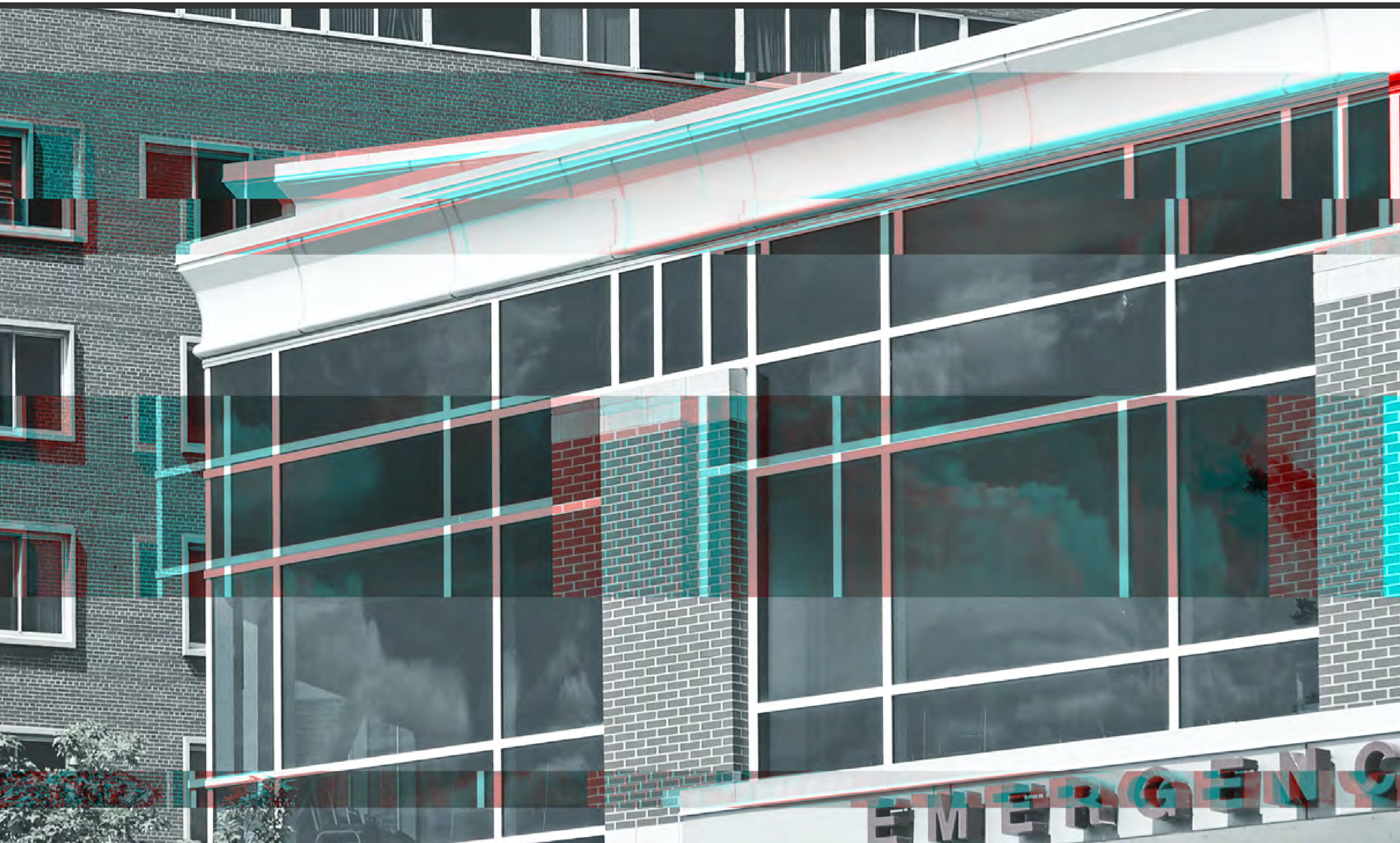


Table of Contents

Introduction

For healthcare IT departments, their responsibilities aren't just numerous. They're in a constant state of change.

With malicious and opportunistic cyberattacks as constant threats, IT teams are expected to protect patient records from being compromised and ensure the organization's infrastructure is stable. They're responsible for guiding internal data security policies and educating personnel on how to prevent breaches. Additionally, they also have to comply with the regulations mandated by the Health Insurance Portability and Accountability Act (HIPAA).

Taking a static "one size fits all" approach to any of these tasks will inevitably lead to problems. As many well-known companies can attest to, taking a reactionary "wait and see" approach to cybersecurity is a good recipe for a data breach and a PR disaster. When it comes to security threats, it's not a question of if, but a question of when.

Balancing the major responsibilities of security and compliance requires a proactive strategy to circumvent problems before they occur. This entails staying current on the HIPAA regulations, on any infrastructure vulnerabilities that widen your attack surface, and on ways to better improve internal procedures to reduce threats.

The usual techniques of firewalls, malware detectors, and encryption techniques can help, but only if they're up-to-date. They must be maintained and monitored by trained staff sophisticated enough to spot real threats in what can be a morass of false positives.

To set the stage for a proactive strategy, a plan will have to be in place for gathering the right knowledge about the importance of HIPAA compliance, understanding the possible threats, and formulating policies on how to protect data while conforming to the necessary regulations.

In the end, an organization can devise a successful means of formulating its best defense by taking the proactive stance of anticipating and seeking to mitigate risks.

The Health Insurance Portability and Accountability Act (HIPAA)

Stolen Payment Cards vs. Stolen Medical Records

Stolen Credit Card Data

= **$1** to criminals

Stolen Healthcare Data

= **$100** to criminals

Source: The Global State of Information Security Survey 2015

In past decades, securing healthcare data was just a matter of ensuring paper files were kept under lock and key in the basement records room.

Today as patient information is being stored in digital form (referred to as electronic patient health information or ePHI), many benefits are now within reach, including access virtually anywhere at any time. Yet sensitive electronic data faces risks that range from attacks by cybercriminals to unintentional mistakes by employees.

To combat these threats or security lapses, the Health Insurance Portability and Accountability Act (HIPAA) was created to make sure that hospitals, clinics, and insurers keep customer information secure from unintended access, in addition to achieving other data security goals.

Enacted in 1996, HIPAA is now an ongoing standard that the health care industry must adhere to, and for healthcare IT departments, the impact is broad and requires a working knowledge of how to best meet the necessary compliance.

Frequency of Healthcare Data Breaches in 2014

1.5/week

Source: Privacy Rights Clearinghouse

HIPAA's security rule offers specifications regarding how to keep sensitive patient data safe while maintaining its integrity and availability. These specifications fall into two categories:

- Required specifications are those that a healthcare organization, known as a covered entity (CE), must meet. Hospitals, clinics and dentist offices are just a few examples of a CE.
- Addressable specifications allow for flexibility regarding how a CE meets the requirement.

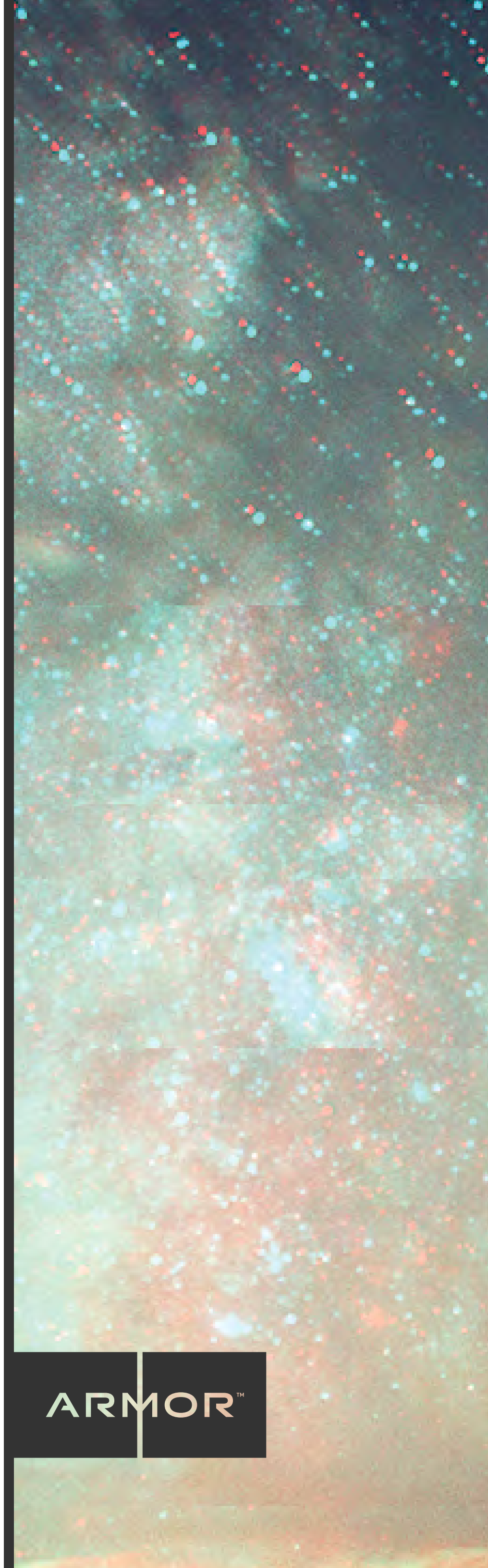
In addition to all the other responsibilities of running a hospital's IT department and solving problems as they occur, meeting HIPAA regulations is a challenging task. It requires taking continual assessments of your IT infrastructure and formulating a plan of action that includes assigning the necessary budget to mitigate the identified risks.

Security is expensive, but, according to Chris Hinkley, senior security architect at Armor, "[it] absolutely is not more expensive than cleaning up a breach."

Such a compromise would likely damage your customer base, your reputation, your sales, and even your stock if you're publicly traded.

"In the basic sense of things," says Hinkley, "security is insurance or a measure of mitigation to prevent that from happening."

When grappling with these issues, understanding how HIPAA has come about can help those who are new to its requirements recognize their importance and why such a national policy was needed to safeguard sensitive data from threats.



The background of HIPAA regulations: “how we got here”

By the mid-1990s, Internet usage had exploded, changing how we communicate and seek out information. As businesses, universities, and government institutions adopted this tech advancement, it was clear that the former system of paper-based record keeping would eventually be overthrown by a digital system.

In anticipation of this inevitability, HIPAA was devised to provide a means for keeping patient data secure and to reduce costs for healthcare organizations.

Before the arrival of HIPAA, no formal privacy standards were in place for protecting medical records. In addition to doctors and nurses, insurance companies and billing clerks had access to patient records without any restrictions on what could be done with that information once it had been accessed. It was clear that any risks to patient information needed to be circumvented through a comprehensive strategy.

It's widely accepted that HIPAA regulations are subjective and open to interpretation. Some experts assert that HIPAA regulations don't go far enough to keep sensitive data secure. The reason behind this nebulousness is because HIPAA regulations were originally designed to be scalable.

This way, the smallest covered entities (such as one-doctor offices) would be just as capable as implementing the standards as New York-Presbyterian Hospital/Weill Cornell Medical Center (which, with 2,259 beds, is cited as the largest hospital in the U.S.[1]).

“With scalability,” says Coalfire's National Healthcare Practice Director Andrew Hicks, “comes vagueness, confusion, and it requires a lot of interpretation.”

> “Before the arrival of HIPAA, no formal privacy standards were in place for protecting medical records.”

Add to this the fact that many small healthcare facilities and SaaS vendors don't have the IT expertise to interpret and fully realize the requirements, and it might seem inevitable that many organizations focus on compliance, leaving deeper security measures unconsidered and therefore not implemented.

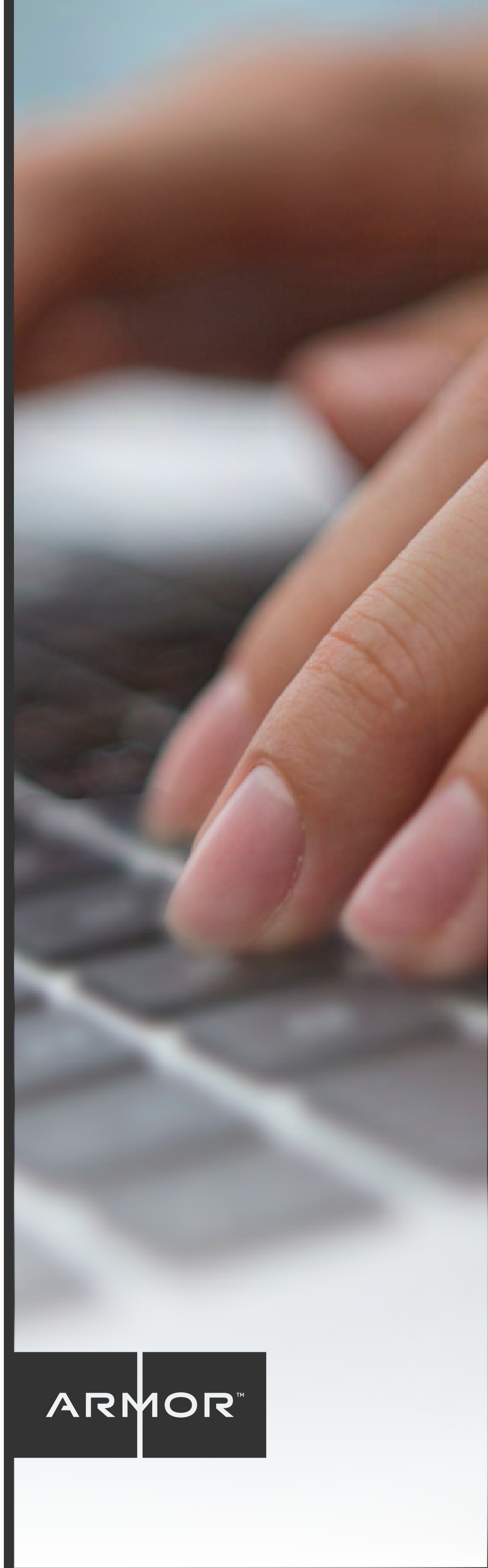
Cyberattacks have not only continued to be a serious threat, but private-sector businesses have experienced massive data breaches in which tens of millions of customer files have been compromised. Maintaining the privacy of patients' healthcare records is one of the goals that HIPAA was created to solve, and its requirements have changed as technology has changed.

The sophistication of the ongoing attacks requires an equally sophisticated approach to security while still providing an easily accessible and user-friendly system that can be used by a large team of employees.

HIPAA has undergone modifications since its first inception to better meet the real-world concerns of both patients and healthcare practitioners. The cloud has also revolutionized how data is shared and stored for hospitals and clinics, causing the IT landscape in the healthcare industry to undergo a variety of changes, including both additional benefits and potential threats.

To avoid data breaches as well as HIPAA penalties, IT experts have needed to become acquainted with the issues of compliance and security, while understanding that equal effort must be devoted to each one.

"To avoid data breaches as well as HIPAA penalties, IT experts have needed to become acquainted with the issues of compliance and security, while understanding that equal effort must be devoted to each one."



Compliance vs. security: both are equally valuable

HIPAA demands not only a conformance to compliance initiatives, but also a comprehensive approach to securing data. The twin issues of compliance and security are priorities for any organization, and both are enormous responsibilities to tackle.

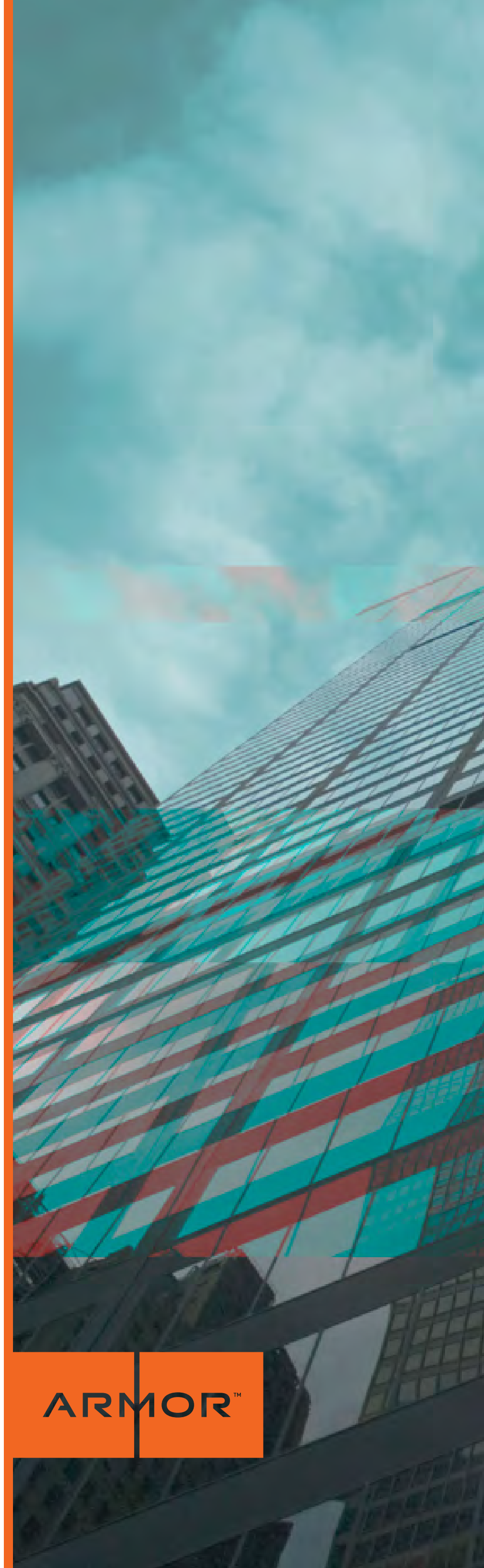
One may seem to have an edge over the other when it comes to importance, yet many organizations have put themselves at risk of being hacked or being penalized by considering one more important than the other. Or they may view compliance and security as being synonymous.

Both carry important distinctions and require different responsibilities. An organization that follows HIPAA regulations to the letter can still be at risk for data breaches since complying with HIPAA doesn't automatically guarantee a secure environment.

Following HIPAA rules will lead to password policies, for instance, and reduce risks that would otherwise be spotted by an audit, but compliance isn't a panacea against hackers or human errors that can lead to compromises.

HIPAA requires password policies to restrict access to sensitive data, but what those policies should look like is left to CEs and their business associates (BAs) to decide.

For example, your password policy could force users to change their password every 90 days, but it might allow them to reset it to the same one. Although this policy technically adheres to the HIPAA requirement, it doesn't conform to strong password standards. That means an organization could pass an Office of Civil Rights (OCR) audit without actually adding much security to their organization.



This is where the Health Information Trust Alliance (HITRUST) has proven to be a valuable partner to any organization navigating compliance and data security issues.

HITRUST is governed by a board of directors comprising leaders from the healthcare industry and its supporters. It provides the Common Security Framework that provides “organizations with the needed structure, detail and clarity relating to information security tailored to the healthcare industry.”[2]

“The HIPAA Security Rule is designed to be flexible and scalable,” says Armor’s Russ Murrell. “As such, the rule provides little direct guidance to Covered Entities (CE) on how to properly secure ePHI. The HITRUST CSF provides a prescriptive approach to securing ePHI by leveraging ‘security best practices’ across multiple security frameworks”.

> “Truly understanding risk management is much more important than compliance.”

Andrew Hicks | National Healthcare Practice Director, Coalfire

For an organization to implement a well-rounded approach that will ensure its operations run smoothly and that patient information is secure, the two pillars of compliance and security must be in place. Although both have equal value, establishing security should be the first item of business, since that will reduce threats of all kinds, and then HIPAA compliance can be built out from there.

“Truly understanding risk management is much more important than compliance,” says Andrew Hicks.
“A comprehensive assessment is more beneficial than chasing the minimalistic compliance requirement.”

It’s up to an organization’s IT specialists to enact such a comprehensive strategy that protects all manner of data before conforming to national standards, and these include establishing encryption techniques.

Have you been sold the wrong kind of encryption?

"As long as data is encrypted, it won't be compromised, right?"

This statement isn't entirely correct and is also a dangerous assumption to make since not all forms of encryption are uniformly the same. Many healthcare organizations consider encryption to be optional, although the truth is that it's actually a mandatory requirement under HIPAA. HIPAA's Security Rule specifies that safeguards be in place to ensure the integrity and confidentiality of ePHI.

It's essential that your security strategy include locating a service that understands HIPAA's encryption standards. Certain encryption formats are stronger than others, and an easily converted type of encryption can be deciphered by hackers with the right tools.

Confusion potentially enters the picture when determining which encryption type is most effective for different scenarios and ensuring the encryption keys are managed properly.

Full-disk encryption (FDE; also known as whole disk encryption) is often used on laptops since it is effective in the case of physical theft. With FDE, a device's entire hard drive is protected as long as the machine is in pre-boot mode — either turned off or before a user can provide authentication credentials to boot up the device.

After a successful boot-up, the data stored on that machine is no longer protected. Subsequently, FDE is not recommended for servers or any device that is on most (if not all) of the time. Logical (or role-based) encryption is more effective when securing data that resides on always-running servers.

> "It's essential that your security strategy include locating a service that understands HIPAA's encryption standards."

Further complicating matters is that the biggest challenge may not lie in the full implementation of encryption (which can be problematic on legacy systems) but in managing the encryption keys and keeping these keys safe. Keys should always be stored in a separate location as the encrypted data without sacrificing convenience to the end user.

A trustworthy vendor will be able to deliver an encryption program that will work in a variety of different settings, through any transportation method, and provide reliable security. A critical component to look for when it comes to encryption is certification, which will convey that a company is a professional and experienced one that can be a trusted partner for your organization.

Certification from the National Institutes of Standards and Technology (NIST) is an established best practice that will deliver a reliable form of encryption cybercriminals won't be able to break easily.

If a CE needs more incentive to take the proper precautions to encrypt data, that incentive can be found in Safe Harbor, a provision under HIPAA's Final Breach Notification Rule.

Safe Harbor frees an organization from the obligation of announcing a breach as long as that organization can prove it has taken the appropriate steps to render that data "unusable, unreadable or indecipherable to unauthorized individuals," according to HIPAA. Organizations also must be able to prove that the encryption keys have been protected.

Business associates must also achieve HIPAA compliance

For the healthcare industry, the definition of a "business associate" (BA) is a person or organization that has access to patient records or handles patient data as part of its services.

A BA often refers to a cloud storage provider that helps guide compliance efforts, but a BA is any third-party vendor that supplies a product or service to a CE. It also must be held to the same HIPAA standards as the CE it works for.

Any data storage a cloud provider performs is vulnerable to unwarranted access or encryption weaknesses unless proper security measures are in place along with meeting compliance standards. To protect an organization and the data it's outsourcing for storage, a business associate agreement will be required under HIPAA.

The OCR has established the minimum requirements that a business associate agreement must entail, and not having one in place would be considered neglect, leading to fines that could total in the tens of thousands. As with any third-party IT service, a service provider has to be chosen wisely since both your operations and reputation will take a massive hit if any sort of data breach takes place.

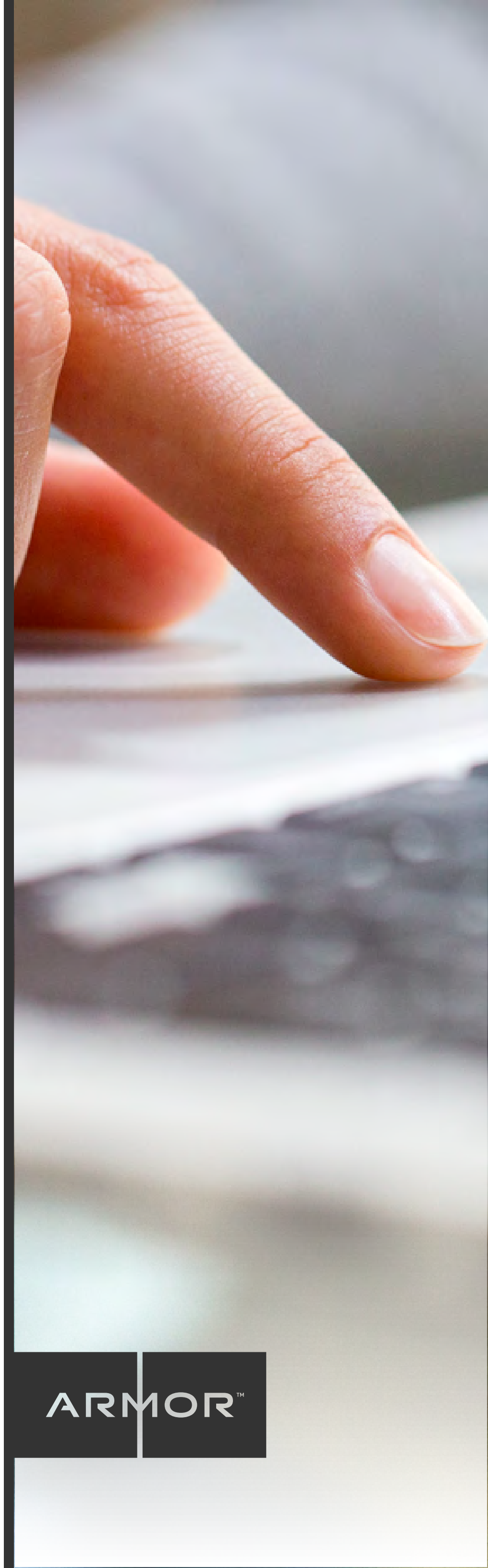
Even if a contract with a BA comes to an end, steps must be taken to cover how any deletion of data is handled to prevent any breaches from occurring. A BA simply agreeing to delete the information won't be good enough. It will need to safely delete any files to prevent any threat of exposure and then provide a certificate of destruction, confirming that the data is completely gone.

A BA can be an excellent ally in your compliance efforts and a helpful resource for allowing your organization's operations to work efficiently. The process for choosing a BA can be compared to choosing a bank; before opening an account, you want to know that the bank employs security guards and utilizes vaults to keep your money safe.

In the same way, a business associate must prove it has safeguards in place. There's no better way for a BA to do that than to achieve HITRUST certification.

"Nobody else can say you're HIPAA-certified," says Hicks. "To achieve this certification, you must have far more controls in place than you do to satisfy the HIPAA requirement."

> "To achieve HITRUST certification, you must have far more controls in place than you do to satisfy the HIPAA requirement."



The costliness of reaction

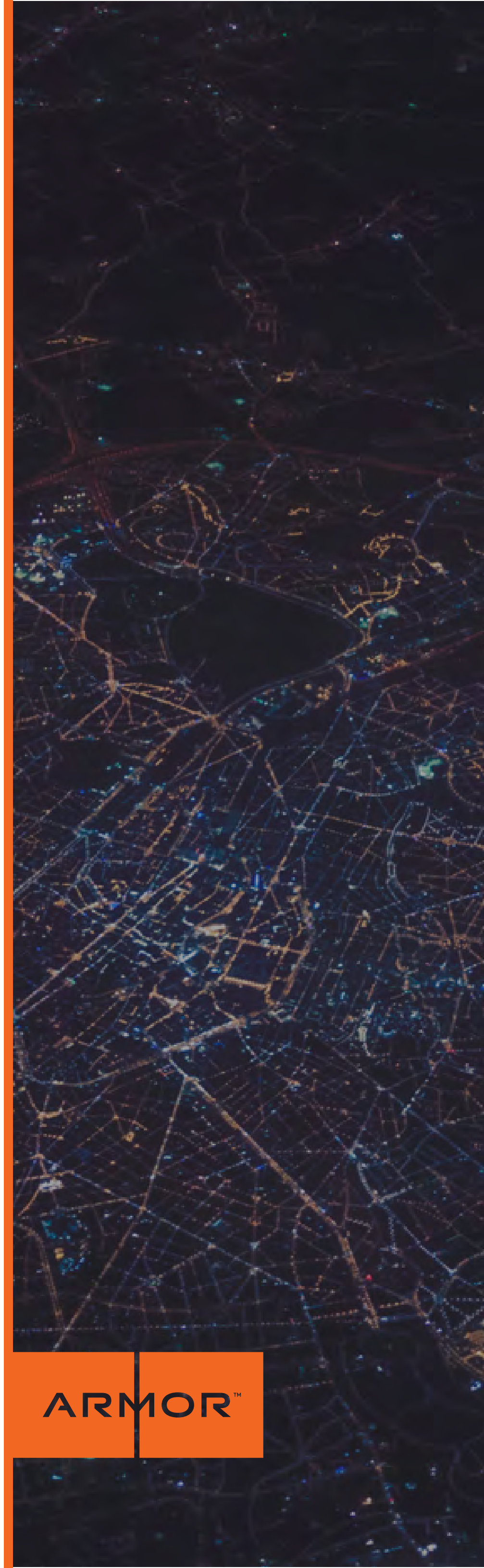
If the first time you consider installing a home security system is after discovering your house has been burglarized, you'll understand the value of being proactive instead of reactionary.

Taking a reaction-based approach to security not only leaves you continually vulnerable to attacks, but you will constantly be devoting time and money to solving problems a proactive approach would help you avoid.

Such a reaction-based pattern is an unsustainable one that will have a variety of different costs that affect not just an organization's operations and revenue, but their reputation as a healthcare provider.

A single instance of a data breach is enough to damage an organization's standing in the community and send the unintended message that it can't be trusted. A data breach that brings an IT system to a halt will have a direct effect on patient care and potentially lead to legal ramifications.

> "Taking a reaction-based approach to security not only leaves you continually vulnerable to attacks, but you will constantly be devoting time and money to solving problems a proactive approach would help you avoid."



Security breaches can also lead to HIPAA fines for not having an effective system in place to protect data. In the rush to install a security patch after a breach, an organization's budget can take a serious hit through the costs of a new protection program and legal penalties.

These financial costs can add up quickly, so devising a plan requires understanding how security and HIPAA overlap and where they diverge. Knowing the budget ramifications of a reactive strategy and the time it eats up is a good place to begin.

> "Which security counter measures you choose to implement depends on what your attack surface looks like."
>
> **Chris Hinkley** | Senior Security Architect, Armor

Companies Cite

$754 BILLION in annual data loss

&

$954 BILLION in downtime

Source: EMC Global Data Protection Index, 2014

Time and money: downtime plus fines

In 2014, the FBI reported that the healthcare community is more vulnerable to data breaches than any other industry.[3] This lack of preparedness is estimated to cost the industry billions over the course of 2015, according to Experian, a global information services company.[4]

Although this is a gigantic price to pay, what is most amazing about it is that these costs can be avoided, provided an organization is following an attentive and comprehensive strategy. As far as the time it would take to find solutions, train employees, and then put the strategies in place, it's estimated that it would require weeks to get an infrastructure up and running again, while still conducting primary healthcare responsibilities.

Last year the Ponemon Institute conducted a study on the cost of a data breach and concluded that for a large organization, it would on average take 31 days to recover from a cyberattack.[5] The total financial cost from that single instance would be roughly $640,000.

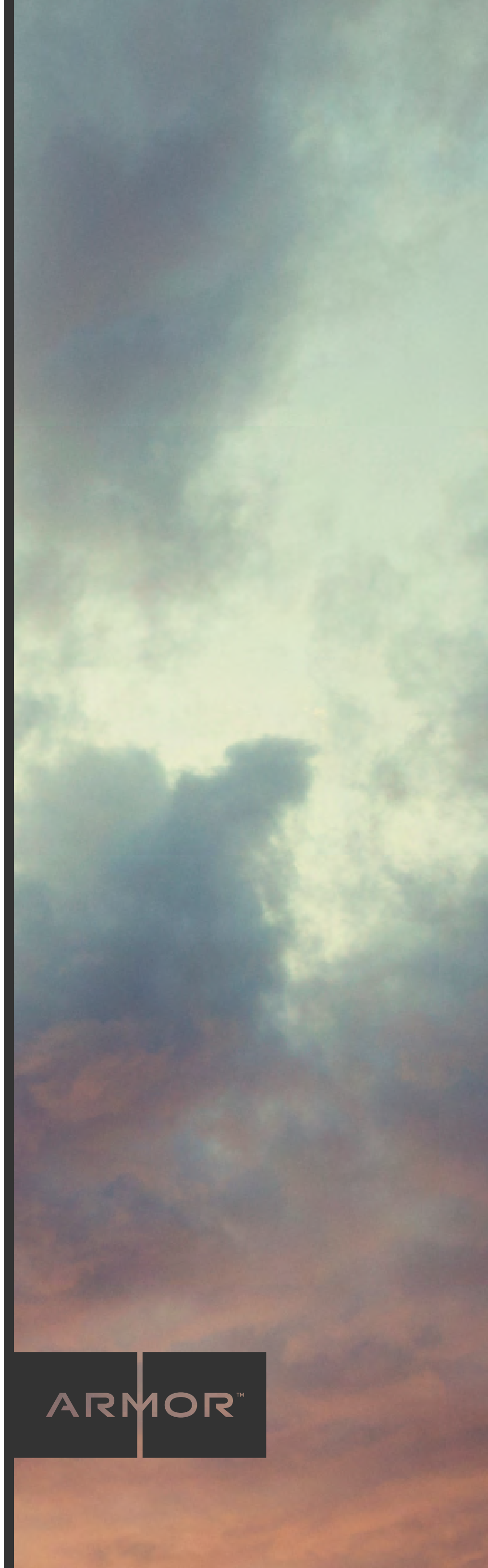
BAs, however, have more to lose from a monetary standpoint than large healthcare systems. Small SaaS companies that partner with CEs often don't have a lot of money set aside to pay fines. Even one data breach resulting in one round of fines can put a BA out of business.

IT downtime can have implications well beyond time and money. For patients who require constant care, a compromised system can have detrimental and life-threatening consequences. Certain procedures may not be able to be monitored or replicated without online systems in action. These situations also affect one crucial factor with far-reaching implications: an organization's reputation.

Breaches by the Numbers

Average spent per year on breaches	$7.6M
Average cost of single data breach	$640,000
Average cost per day	$20,000
Average times an organization is breached	122

Source: 2014 Cost of Data Breach Study, Ponemon Institute LLC



Reputation: loss of trust or customers

Any business seeks to establish trust with a consumer. Without it, no relationship will even exist, and for a healthcare provider, this sense of trust can have a greater meaning than for a private-sector business.

Not only is data being maintained, but the healthcare provider is also responsible for delivering actual care, including restorative treatments, surgery, and wellness practices.

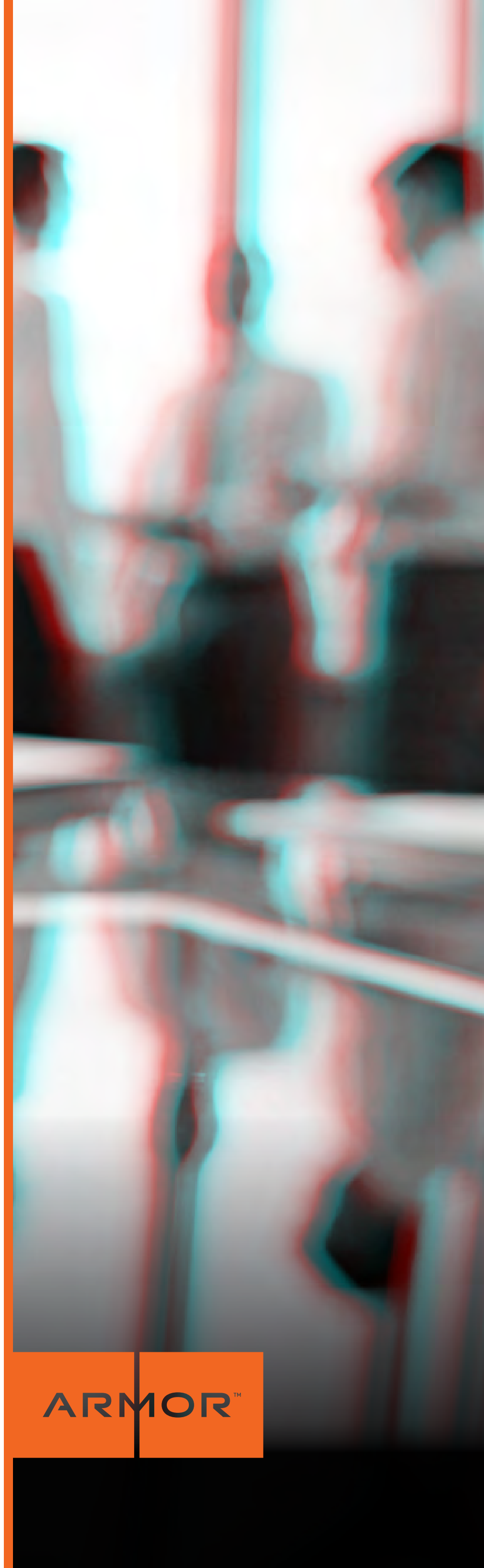
Yet hospitals don't have the same concerns about a damaged reputation that other businesses do because people still must go to the hospital if they're injured or sick. As with fines levied due to a breach, losing trust is often a larger concern for BAs, who depend on an impeccable reputation to remain in good standing with their customers — the hospitals, healthcare clinics and other CEs.

A BA who allows a breach to happen is likely to be fired by the CE who has hired them and will suffer other losses from that damaged reputation.

Taking a proactive approach to security, including the steps necessary to achieve Safe Harbor status, can greatly reduce the chance of having to face this kind of situation.

A central facet in that approach is being able to reasonably assess the spectrum of risks that hospitals, vendors, and service providers face and then devising a risk management strategy for mitigating them.

"Which security countermeasures you choose to implement," Chris Hinkley of Armor explains, "depends on what your attack surface looks like, which determines what mitigation looks like."



Risk assessment and management

Security emergencies can result from a variety of different sources, yet it's impossible to plan for all of them. Even with a strong infrastructure and a well-trained staff, no one is immune from attacks, and it's important to consider the many potential security vulnerabilities facing an organization and those of its BAs.

The only way to do that is to conduct a comprehensive risk assessment that takes a hard look at your organization, sizes up its attack surface, and identifies vulnerabilities, many of which you may not even be aware exist.

A comprehensive risk assessment, Andrew Hicks of Coalfire says, must probe into "every channel, every person, and all systems that interact with the ePHI data." A requirement of security, he explains, is "knowing where the data is and how it is accessed, how it flows through your systems."

So an integral part of the risk assessment is the process of discovery. As has often happened with an IT team focused on their own goals, the business might be engaging in activity that the IT team doesn't know about.

By 2016,

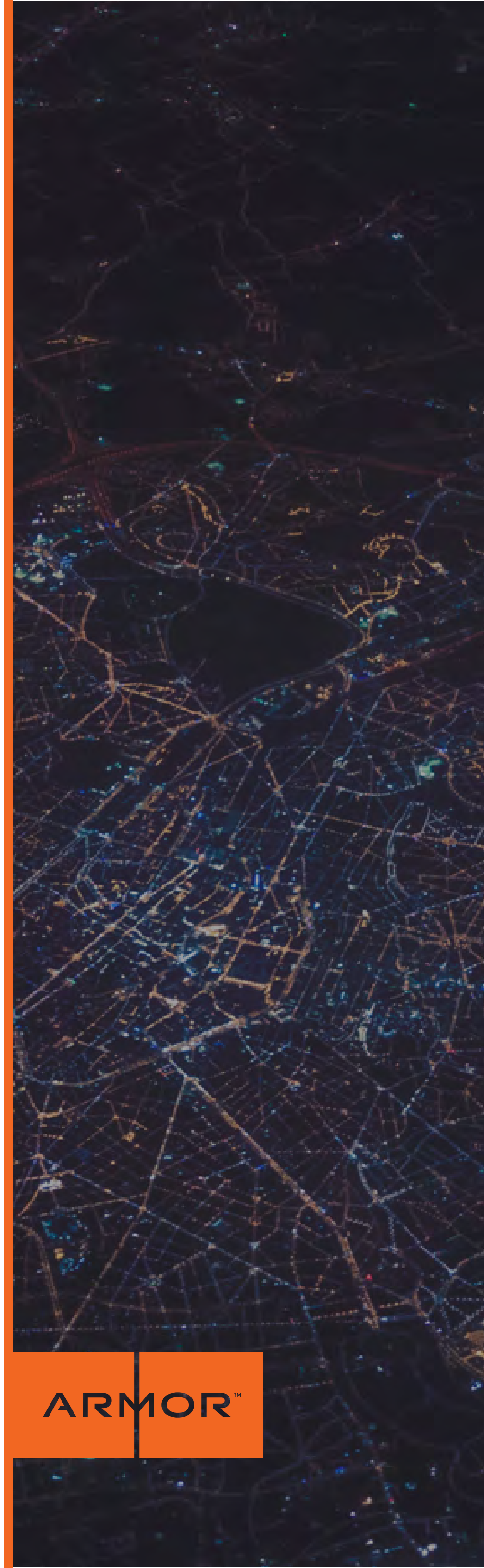
80%

of reported security failures will be due to:

Lack of risk assessments

Poor governance

Source: Axway infographic: The Road to HIPAA Compliance



The business must be brought into the discovery process to collaborate with IT to fully and properly assess your risks. This can lead to an arduous and painful yet absolutely necessary process of learning what you don't know about how your data is handled and accessed.

"It is clear that that malicious actors, including both cyber-criminal groups and state-sponsored hackers, have set their sights on healthcare companies," says Russ Murrell or Armor. "The business and IT leaders need to be ever-vigilant in re-assessing the risk posture."

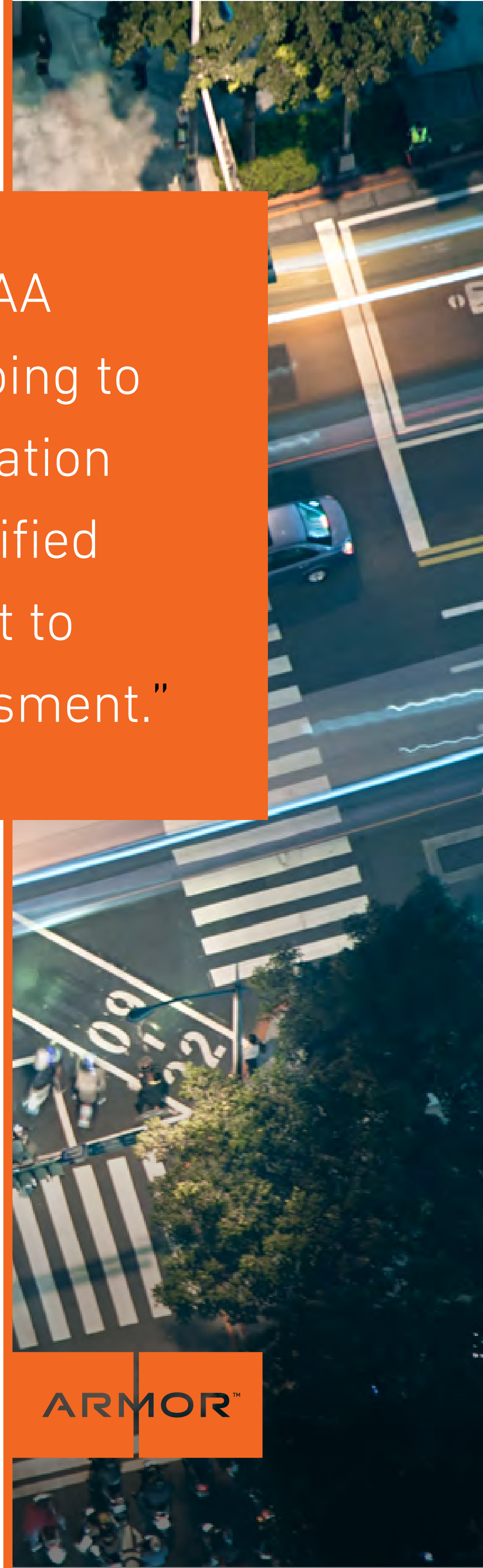
This is where having a third-party vendor experienced with conducting thorough risk assessments is a valuable option. A team with the right experience will not only offer much-needed subjectivity to the risk assessment process, but also help you ask the right questions.

You must uncover exactly who is accessing data, as well as where and how (are mobile devices and external hard drives properly secured?). You'll also need to classify your servers (whether or not each contains ePHI) and determine which irregularities (such as undocumented workarounds) that employees have devised to get the job done.

The following sections outline some major risks to be aware of when conducting a risk management assessment, as well as tips for mitigating those risks.

> "When you look at the HIPAA rule, it says that you're going to protect the health information from all reasonably identified threats. The starting point to doing that is a risk assessment."

Kurt Hagerman | CISO, Armor



External attacks

Healthcare data is some of the most under-protected information online, and any organization that doesn't take hacking threats seriously is setting a trap for its operations and integrity.

"There's no such thing as an impenetrable fortress for a network environment," remarks Mac McMillan of CynergisTek. "You have to accept that you can be violated."

Data that's entered from employees on an in-house system is a major target, and many devices that produce information aren't protected at all from attacks. Many threats are often opportunistic in nature, such as a break-in to a weak system, something that many would-be invaders scan the Internet looking for. Other external threats include malware invasions and password thefts.

> "A risk assessment should entail every channel, every person, all systems that are interacting with your ePHI data."

Andrew Hicks | National Healthcare Practice Director, Coalfire

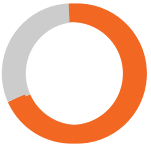
Tips for Prevention

- Far too many healthcare institutions don't have a strong protection system at work. Implementing a thorough and sophisticated security strategy can help decrease your attack surface, making you less desirable to the lazy cybercriminal looking for low-hanging fruit to snatch.
- By hiring a team of IT experts who can continually locate vulnerabilities, you can keep your infrastructure and data out of the reach of dedicated cybercriminals. An organization will also need to undergo risk assessments under HIPAA regulations. It's recommended that the assessments be subjective and conducted on a regular basis.

Employee errors

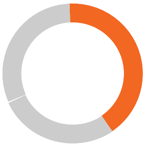
The current statistics report that a large percentage of data breaches come from inside an organization through unintended employee mistakes, such as mishandling data. These stats are also consistently growing from one year to another, proving that not enough is being done to prevent these costly and potentially disastrous mistakes. "The bad guys count on user error — on human error," explains McMillan.

Biggest threats to data security: employee negligence



69%

Employee behavior (a combination of mistakes, lax access controls, and malicious activity)



39%

Unintended mistakes by internal staff (making this the leading overall cause of data breaches)

Source: "Leading Cause of Data Security Breaches Are Due to Insiders, Not Outsiders," PR Newswire

Tips for Prevention

- Training has to be at the heart of any risk management endeavor, and it must be an ongoing process. By providing ongoing training in security and risk mitigation measures, you'll send the message that you take security seriously. Empowering all staff to play a part in helping an organization be more secure is about building a culture of security in which everyone understands the risks and how to help mitigate those risks.
- Give staff an awareness of the threats out there and some hands-on training so that they know how to react to different scenarios. People should be made aware that confidential information attached to an email can end up with the wrong recipient and that passwords should be strong and not easy to break.
- Take a hard look at how you're allowing data to be handled and identify ways to mitigate the unintentional (or malicious and intentional) mishandling of data. For example, setting a limit on how much data can be exfiltrated at one time can help control where the data is going and why.

System glitches

Sometimes when a problem occurs, it's the technology that's to blame. Right behind employee errors, system glitches are a frequent reason for data breaches. A system glitch can take many different forms without much indication that it's about to occur.

A large enterprise's IT infrastructure will undergo a great deal of traffic around the clock, and delays or slowdowns can be a major hindrance to operations.

Tip for Prevention

- Assess your infrastructure periodically to monitor when further growth is necessary to keep the system robust enough to handle its data needs. Bugs will inevitably occur after software has been deployed, and instituting a strategy for handling problems will allow an organization to be prepared in case a crisis occurs.
- Expecting that nothing will go wrong will only leave you scrambling for a solution when a problem occurs, causing costly delays. Identify risks as part of your assessment phase, and implement a risk management plan that seeks to mitigate those risks as comprehensively as possible.
- You need the right tools and technology, but you also need the right people monitoring and maintaining those tools. Breaches are often difficult to detect, Hagerman explains, because "organizations don't have sophisticated enough monitoring systems in place and the right staff watching all the time to understand which behavior is anomalous."

Business associate errors

BAs can be seen as an extension of your workforce, and just as internal employees can make mistakes that lead to major security problems, third-party vendors have the potential to do the same.

According to Hicks, many BAs are failing to understand the risk management aspect.

“There’s so much to compliance than just following the checklist. Doing that comprehensive evaluation,” he emphasizes, “is more valuable than chasing the minimalistic compliance requirement.”

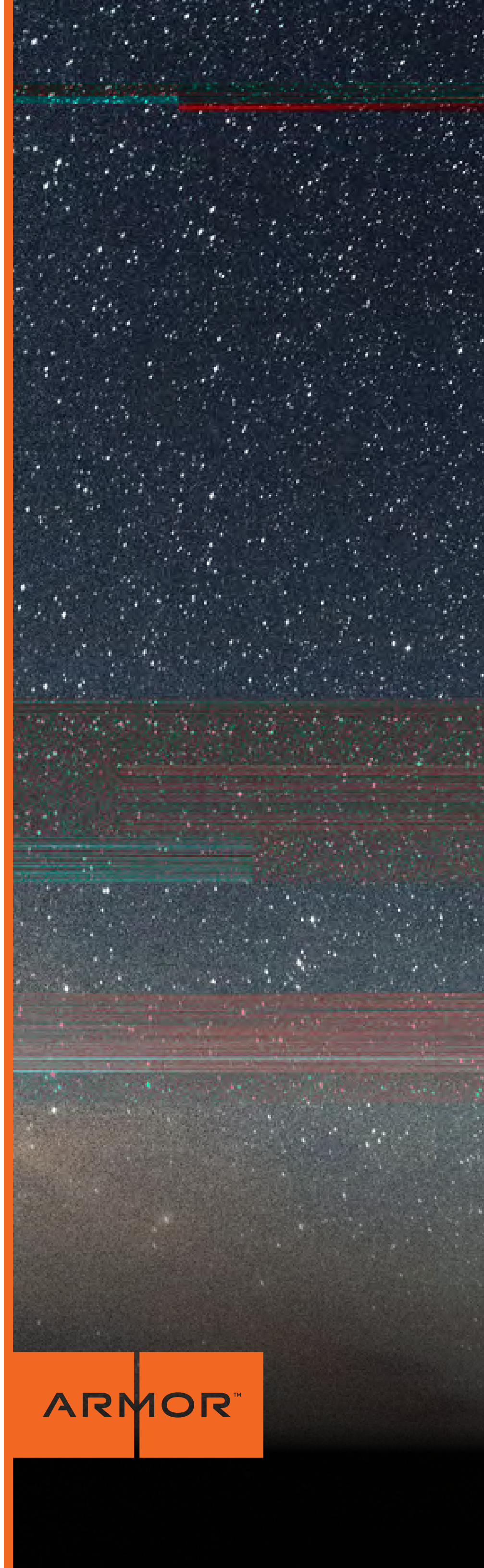
By conducting a risk assessment, you’ll be able to lay the groundwork for new security procedures, a training program for employees, and requirements for BAs who handle or store patient or employee data.

This process can pinpoint current vulnerabilities and future ones, allowing a proactive policy to begin and become part of company processes. A culture of responsibility and awareness can play a huge role in eliminating many security problems and engender a greater sense of safety among team members.

Tips for Prevention

- When choosing a dependable BA, you should ask them a series of security-related questions to determine how dependable and knowledgeable they are when it comes to preventing data breaches.

  Certain providers will not only be trustworthy, but they may be able to guide a healthcare IT department through the process of creating a stronger infrastructure that also meets HIPAA’s standards.



Proactive do’s vs. Reactive don’ts

Whatever the size of an organization, the price of a data breach will be far more expensive than the costs of creating a strong infrastructure with different layers of protection in place.

Taking a proactive approach will help an organization avoid most threats and keep company operations running efficiently, rather than waiting around for a strike to occur before a reactionary strategy is devised. Here are some essential actionable tactics to take and some reactionary mistakes to avoid.

75%

of all cyberattacks are opportunistic

Source: Industry Leadership Tip Card, Department of Homeland Security

> “Security professionals have to be right 100 percent of the time. An attacker only has to be right once.”

Chris Hinkley | Senior Security Architect, Armor

Proactive do's

Do encourage a culture of security.

Make sure employees know how data breaches can occur and the steps they can take to prevent security problems. By promoting safety practices, risks can be greatly reduced in a way that is cost effective and lays the groundwork for other proactive practices.

Do conduct a proper risk assessment.

Certain vulnerabilities may be expected, yet unforeseen weaknesses may be lurking that your organization won't know about unless a risk assessment takes place. These assessments should also be conducted on a regular basis to stay a step ahead of the threat actors.

Do encrypt your data the right way.

Not all encryption is the same, so it's crucial that your organization use the right techniques in the right scenarios. Outside the confines of your infrastructure, you'll also need to ensure that any BAs are utilizing effective encryption methods.

Do patch your system.

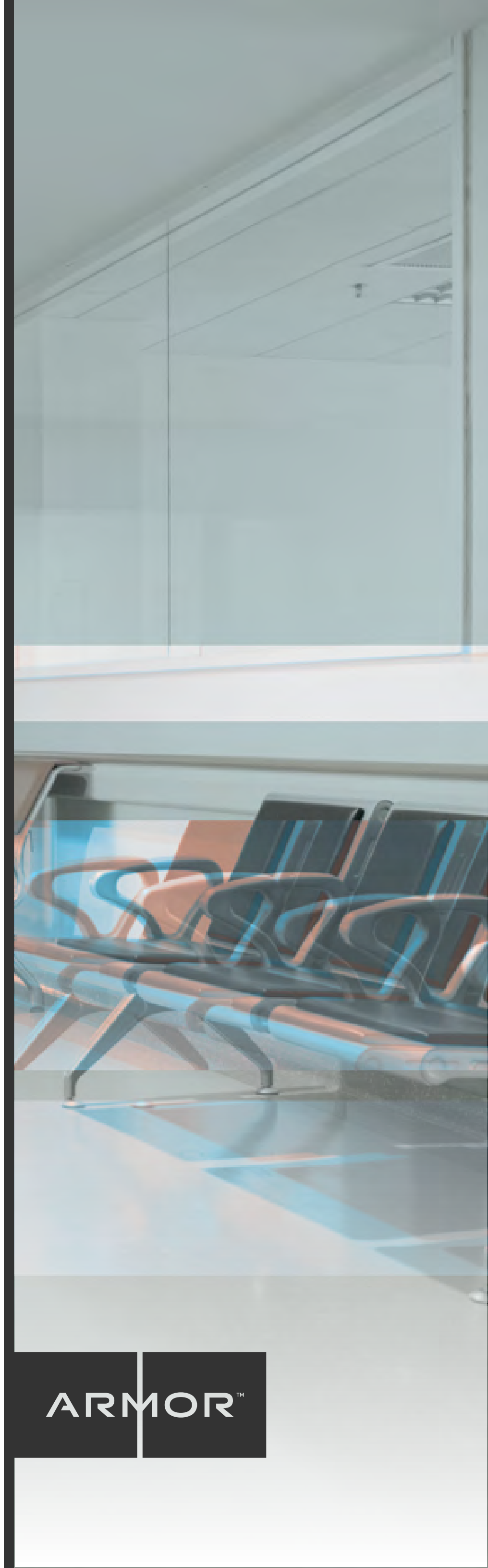
What's secure today will be open to an attack tomorrow, and even the strongest system eventually will run into problems. When weaknesses are spotted, implementing patches will be necessary and should be conducted immediately as a top priority.

Do monitor your system.

Taking a proactive approach to security means keeping an eye on your infrastructure so you can devise an appropriate defense strategy and know the tactics hackers are using. Also ensure your team knows the difference between normal and abnormal behavior on the system.

Do get the right people in place and ensure they have the proper training.

A knowledgeable IT team will be the foundation for all of an organization's security and compliance efforts. By assembling a group with the necessary skills, your organization will have a way to stay current on the latest security measures and help prevent future attacks.



Reactive don'ts

Don't sacrifice security in favor of compliance.

Trying to comply with HIPAA may seem like a greater priority than overall security, and that it will cover many security issues, but one shouldn't be seen as more important than the other. Neglecting security can lead to a complete take-down of your system, and procrastinating on compliance can lead to costly fines.

Don't ignore potential vulnerabilities that widen your attack surface and leave you open to opportunistic criminals.

No matter how small the exposure, any vulnerability still offers the potential for a breach that could lead to huge consequences. Household names have allowed weaknesses in their infrastructure to put them on the front page of the paper by giving hackers an opportunity to wreak havoc.

Don't wait for a breach to happen to you before you decide to take action.

Taking a reactive approach to security will be costly for your organization in terms of finances, productivity, and reputation. If you're fortunate enough to be free from a data breach, don't expect that this trend will continue. The only way to reduce risks will be to take a proactive approach and begin implementing thorough security and compliance policies.

Don't consider security and compliance to be the same thing.

These aren't synonymous terms, as each one covers different issues. Although experts recommend tackling security first, both have to be given equal effort.

Don't assume a secure infrastructure will last forever.

Don't allow your IT infrastructure to become vulnerable through a lack of updates or upgrades. A system will have to be continually updated to ensure data is protected and that threats are reduced.

Don't take on all these responsibilities without guidance.

Keeping a healthcare institution's system up and running is a huge task even without factoring in HIPAA compliance and overall data security. Receiving guidance from an experienced compliance expert can go a long way toward helping avoid penalties and security breaches.

Conclusion

Don't wait for the bad guys to find you.

"Every organization can be breached," cautions CynergisTek's McMillan, because "there's no such thing as an impenetrable fortress for a network environment."

Taking a multifaceted and proactive approach will help you build an environment that makes security a priority.

As Armor's Hinkley recommends, "Protect, detect, respond: Protect first. If I can't protect, then detect. Then respond to the detection alert."

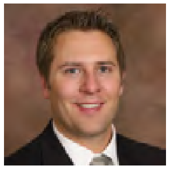
No matter the size of your organization, security and compliance challenges are an ongoing battle, and the time to start fighting is now.

Security Priorities

- Create internal policies that help your staff understand the importance of security and the part each team member plays.
- Stay current with security updates and patches to keep up with threats that constantly evolve.
- Develop a plan that regularly identifies potential vulnerabilities in your attack surface.
- Prioritize security efforts and implement effective counter-measures to mitigate the risks.

Acknowledgments

Armor would like to thank each of the interviewees for their contributions of time and expertise in helping shape this project.



Andrew Hicks
National Healthcare Practice Director, Coalfire

Mac McMillan, FHIMSS/CISM
Chairman & CEO, CynergisTek

Kurt Hagerman
CISO, Armor

Chris Hinkley
Senior Security Architect, Armor

Russ Murrell
Security & Technology Strategist, Armor

Sources cited

1. “100 largest hospitals in America,” http://www.beckershospitalreview.com/lists/8-7-14-100-largest-hospitals-in-america.html

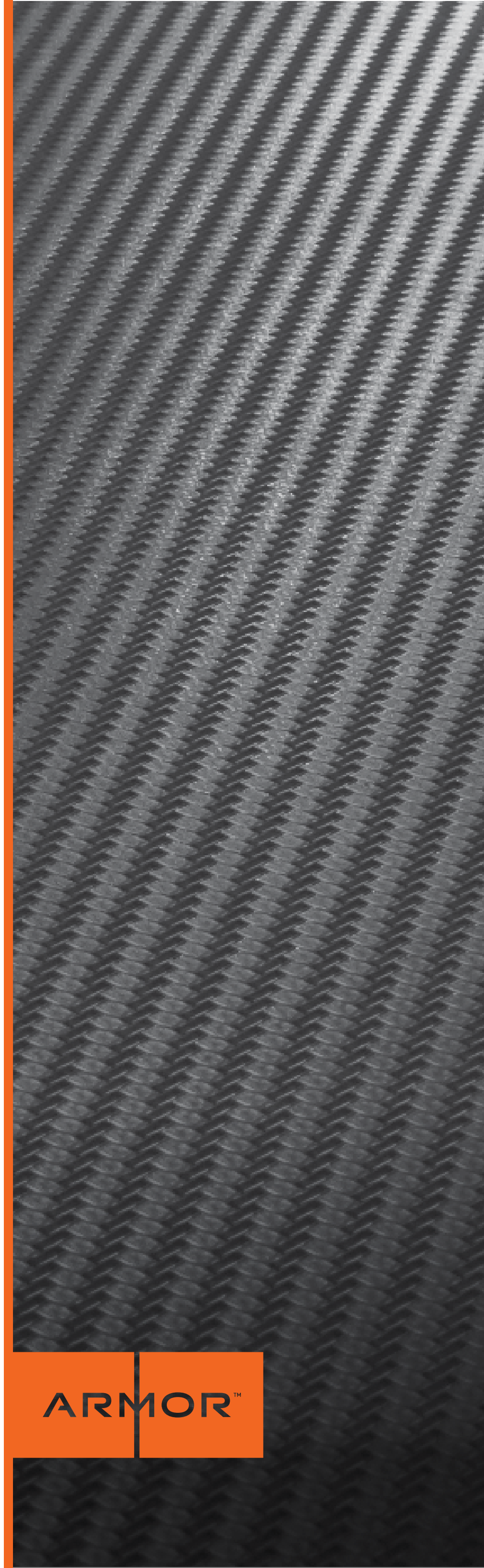
2. https://hitrustalliance.net/about-us/

3. “Exclusive: FBI warns healthcare sector vulnerable to cyber attacks.” http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423

4. 2015 Second Annual Data Breach Industry Forecast. http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182

5. “Data Breach Costs Rise 23%.” http://www.seculert.com/blog/2014/11/data-breach-costs-rise-23.html

Copyright



US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™

BETWEEN YOU AND THE THREAT